SCIS'99 The 1999 Symposium on
Cryptography and Information Security
Kobe, Japan, January 26-29, 1999
The Institute of Electronics,
Information and Communication Engineers

# MPEGストリームから検出可能な動画像電子透かし方式の検討

# A Note on Watermarking Method for Moving Picture to Extract from MPEG Bitstream

酒澤茂之* 羽田知史* 滝嶋康弘* 和田正裕*

Shigeyuki SAKAZAWA Satoshi HADA Yasuhiro TAKISHIMA and Masahiro WADA

KDD 研究所

KDD R&D Laboratories

あらまし DCT係数の操作に基づく電子透かし方式を提案する。動画像を対象とするために、提案方式では各画像フレームには簡易な方式で透かしを埋め込み、その検出精度の低さや情報容量の少なさの欠点を複数の画像フレームを利用することで解決している。このとき、透かし抽出に用いるフレーム数を増やすほど精度や情報容量を増やせるというスケーラビリティを実現している。また、提案方式はMPEG で圧縮されたビットストリームを復号することなく透かし抽出が可能であるという特徴を有する。計算機シミュレーションにより、MPEG による圧縮の影響を受けることなく透かしを保持可能であることを示す。

キーワード 電子透かし、MPEG、スケーラビリティ、統計的抽出

## 1. はじめに

デジタル放送や DVD など映像コンテンツのデジタル流通が進められようとしている。こうしたコンテンツ流通をビジネスとして成立させていくためには著作権保護を保証することが必須条件であり、その中で電子透かし技術はコンテンツの不正利用を抑止するための技術として重要である。

電子透かしに要求される機能要件としては、透かしが視認されない秘匿性、透かしが容易に除去されない耐攻撃性、数 10 ビット程度の情報が埋め込める情報容量など[1]がある。動画像に透かしを埋め込む際には、上記の要件に加えていくつか考慮すべきことがある。それは、第一に画像フレーム数の多さである。例えば、2 時間の動画像であれば 10 万以上のフレーム数となるため、処理対象フレームの選択や演算量の観点で配慮が必要となる。また、動画像が流通される場合には、その膨大な情報量を圧縮するために MPEG が用いられることが確実である。従って、圧縮された MPEG ストリームの状態から復号することなく電子透かしを抽出できることが望ましい。また、当然のことながら MPEG 圧縮によって透かしが消えないことが必要条件となる。

本稿では、まず従来の静止画像を対象とした方式を動画像に適用した場合の問題点について検討する。そして、その検討に基づいて、新しい統計的処理による電子透かしの埋め込み・抽出方式を提案する。本方式は DCT を用いた方式であり、同じく DCT を用いる MPEG ストリームを復号することなく電子透かしの抽出が可能という特徴を有する。そして、提案方式が MPEG 圧縮によって受ける影響を検証する。

## 2. 静止画像透かし方式の考察

静止画像を対象とした電子透かし方式は、振幅、周波数、位相を変調する方式に大別される。これ

* KDD 研究所 〒356-8502 埼玉県上福岡市大原 2-1-15
KDD R&D Labs., 2-1-15 Ohara Kamifukuoka-shi, Saitama 356-8502, Japan

らのうち、耐攻撃性と情報容量の観点から実用的と思われる方式は、直交変換の低周波成分の利用[2]、スペクトル拡散法の利用[3]である。他にも、情報容量の点では難があるものの優れた方式として、フーリエ変換の実数部と虚数部の位相をずらす方式[4]もある。

動画像を対象とするとき、これらの方式を適用する最も単純な方法は、全画像フレームに対して同じ透かしを埋め込むものである。このとき、透かしの検査者は任意の画像フレームを取り出してきて検査すれば良い。欠点としては、すべての画像フレームに同じ情報が埋め込まれるため耐攻撃性が弱まる恐れのあることと、処理対象の画像フレーム数が多いため演算量が膨大となることである。耐攻撃性については、フレーム位置によって埋め込む情報を変更・変調することにより改善されるが、情報の抽出にあたり当該フレームの位置情報が必要になる可能性がある。

次に、動画像系列中から特定のフレームを選択し、そのフレームだけに透かしを埋め込む方式が考えられる。この方式では透かし埋め込み処理は軽いものの、検査者は膨大な動画像系列の中からこの特定のフレームを見つけなくてはならなくなる。しかし、この位置情報をア・プリオリに持つことは不可能である。たとえば先頭から 100 フレーム目に埋め込んだとしても、編集によって容易にその位置は変更され得る。よって、この方式には位置情報をいかに保持するかという問題がある。

なお、原画像を透かし抽出に用いる方式も同じ問題を持つ。これは、検査対象の画像系列と原画像系列のどのフレームが対応するかを判定しなければならないため、位置情報が必要になることによる。

上記の考察により、動画像に透かしを埋め込む際には、全フレームに対して軽い処理で埋め込み・抽出ができること、および位置情報を得るための「同期」メカニズムが必要になると思われる。ただし、一般に簡単な処理で埋め込んだ場合には耐攻撃性や情報容量の点で不十分になると予想される。そこで、透かしを多くのフレームに渡って薄く広く埋め込むことが必要になる。この処理フレーム数を増やすほど抽出情報量をことができ、かつ情報の確実性も向上するスケーラビリティ的な考え方を導入するべる。なお、透かし埋め込み方式としては、Iースとすることで、MPEG で用いられる動DCT 符号化方式と親和性が確保され、MPEすることなくビットストリーム上で透かし可能になると期待される。

## 3. 提案方式

本方式では、画像フレーム中の DCT ブロ一つ選択し、その係数値を変化させることに埋め込みを行う。このとき、選択した DCT クの位置が秘密情報となり、その位置におめ込みの有無によって透かし情報を表現すの埋め込み方法を用いて、透かし情報を 2 階造により原画像系列に埋め込む。第 1 階層にしの存在判定および同期フレーム構成に用いる。第 2 階層は同期フレームに基づいて、更情報埋め込み・抽出のために用いられる。

### 3.1 DCT係数への埋め込みと抽出

原画像フレーム（輝度信号）を 8×8 画素にし、そのうちの一つを選んで DCT を施す。そ(1)式に基づいて、ある固定の DCT 係数の値対値が大きくなる方向に変化させ、逆 DCT をて画像に戻す。

$$x' = sign(x) \times (|x| + a) \qquad (1)$$

x は元の係数値、a は埋め込み値、sign(x)は x 号を与える。

埋め込みの有無の判定は、MPEG のマクロック(MB)の単位で行う。MPEG では 4 つの I ブロックからなる MB の単位で符号化・復号うため、1 つの MB には 1 つの埋め込み DCT ックと 3 つの非埋め込み DCT ブロックが含まそこで、埋め込みブロックの係数値とそれ以外ブロックの平均値との偏差によって、埋め込有無を判定することができる。

$(|x_1| + |x_2| + |x_3|)/3 + s < |x|$ ならば埋め込み有り

x は埋め込み DCT ブロックの係数値。$x_1, x_2, x_3$

それ以外のブロックの係数値。sは$|x_1|,|x_2|,|x_3|$の標準偏差

ここで、上記のDCT係数埋め込み方式では必ずしも100%確実に抽出できないので、複数のサンプルについて検査し、統計的に埋め込みの有無を判定する必要がある。

なお、MPEGで圧縮されたビットストリーム上で判定する場合には、動き補償の復号は行わず、ハフマン復号して得られるDCT係数値のみを用いる。したがって、フレーム間予測のみでDCT係数を含まないブロック（not-Coded ブロック）については、判定を行うことはできない。

### 3.2 第1階層の埋め込み・抽出

位置情報の復元のためにN画像フレームを用いて同期をとる。そのために、図1に示すように画像フレームごとに埋め込むDCTブロックの位置を変えていき、Nフレーム周期で埋め込み位置が一周するよう埋め込みを行う。この埋め込み位置情報をテンプレートと呼ぶこととし、秘密情報として保持する。

抽出を行う際には、テンプレートを動画像に対して1フレームずつずらして適用し、全部でNとおりの場合について埋め込み判定を行う。そして、埋め込み有りと判定されたフレーム数の確率が最も大きくなったテンプレート位置に基づいて同期を回復する。なお、埋め込み判定が決定論的なものではなく、確率論的なものであるため、検査フレーム数を長くとることで精度を高められる。このとき、テンプレートのNフレーム周期に関係なく、任意の長さの画像フレームにわたって検査を実施してよい。ここで、MPEGビットストリーム上で抽出を行う場合には、not-Coded ブロックは埋め込みフレーム数の確率の計算から除外する。

### 3.3 第2階層の埋め込み・抽出

前節で構成したNフレーム周期の起点に基づいて、Nビット情報埋め込みを行う。図2に示すように、動画像シーケンスをNフレームでインタリーブし、その第1フレームグループについて、あ

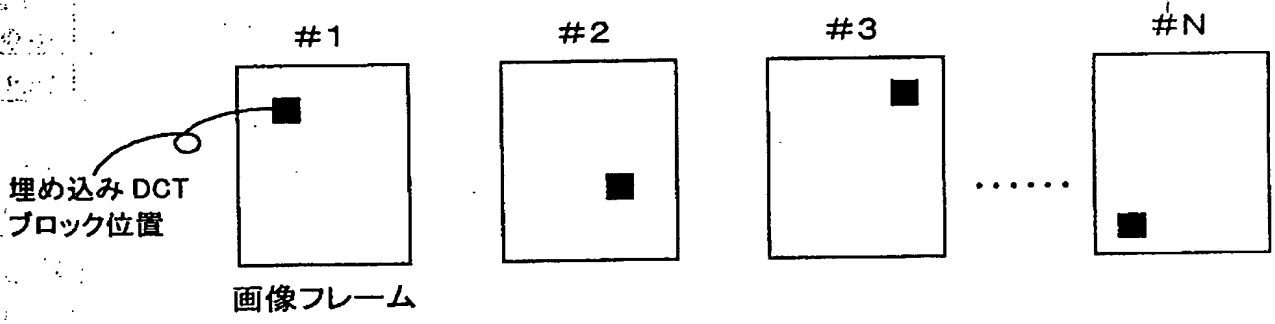


図1　第1階層埋め込みテンプレート

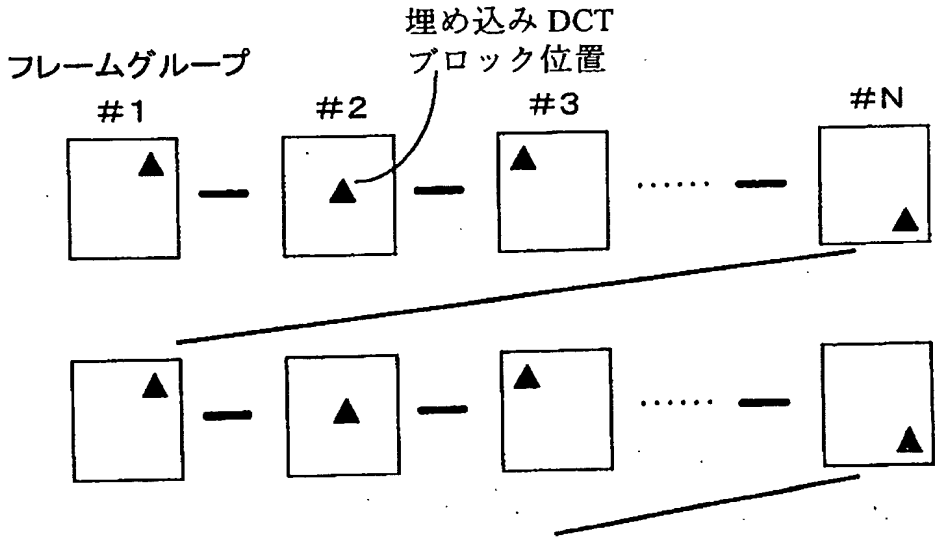


図2　第2階層埋め込み

る位置のDCTブロックを第2階層用の埋め込み対象とし、第2フレームグループについてはまた別のDCTブロックを埋め込み対象とし、これを第Nフレームグループまで行う。このとき、フレームグループごとに1または0の1ビット情報を埋め込むことができる。すなわち、第1フレームグループに対して情報ビット1を埋め込む場合には、グループ内の全画像フレームの埋め込み対象DCTブロックに対して埋め込みを行う。逆に情報ビット0を意味させるときには、埋め込み対象DCTブロックに対して埋め込みを行わない。このようにしてフレームグループごとに独立に1または0を埋め込むことで全体としてNビットの情報を埋め込むことができる。

本方式の拡張として、フレームグループごとに2個所のDCTブロックを埋め込み対象とすることで2Nビットの埋め込みができる。また、フレームグループ内で第1階層で用いたのと同様のテンプレートによってDCTブロック位置を周期的に変えることによりセキュリティ強度や抽出精度を向上させることができる。

抽出については、フレームグループごとに1か0の多数決判定によって行う。第1階層での抽出と同じく、MPEGビットストリーム上で抽出を行う場合には、not-Codedブロックは埋め込みフレーム数の確率の計算から除外する。

## 4. 計算機シミュレーション

提案方式においては、DCTブロックへの埋め込みの検出精度が第1および第2階層の検出精度の元になるため、その検証を最初に行う。

DCTブロックの埋め込み検出における誤り確率は、埋め込みDCTブロックの検出に失敗する消失確率と、非埋め込みDCTブロックを埋め込みDCTブロックと誤って判定する誤検出率とからなる。そこで、以下のシミュレーション条件における各確率を調べる。

| | |
|---|---|
| 動画像 | FlowerGarden, Bicycle, Susie (720画素 x 480ライン x 29.97Hz) 150フレーム |
| 埋め込みDCT係数 | 第(0, 3)係数 |
| 埋め込みブロック | 選択されたMB中の左上のブロック |
| 符号化アルゴリズム | MPEG-2 TM5[5] (N=15, M=IBBPBBP...) フレームストクチャ |
| 符号化ビットレート | 15, 8, 4 Mbit/s |

埋め込み値はMBごとに視覚的に目立たない値とした。

表1　透かしの消失確率と誤検出率(%)
(MPEGビットストリーム)

| 画像/MB座標/埋め込み値 | 種別 | ﾋﾞｯﾄﾚｰﾄ(Mbit/s) | | |
|---|---|---|---|---|
| | | 15 | 8 | 4 |
| Flower/(23,10)屋根/50 | 消失 | 15.2 | 12.3 | 13.3 |
| | 誤検出 | 14.4 | 25.0 | 7.1 |
| Bicycle/(39,5)林/50 | 消失 | 11.8 | 13.0 | 26.5 |
| | 誤検出 | 25.7 | 22.4 | 18.2 |
| Susie/(26,10)右頬/10 | 消失 | 12.0 | 20.3 | 18.0 |
| | 誤検出 | 18.8 | 20.5 | 18.2 |

表2　透かしの消失確率と誤検出率(%)
(MPEG復号後)

| 画像/MB座標/埋め込み値 | 種別 | ﾋﾞｯﾄﾚｰﾄ(Mbit/s) | | |
|---|---|---|---|---|
| | | 15 | 8 | 4 |
| Flower/(23,10)屋根/50 | 消失 | 12.0 | 12.7 | 15.3 |
| | 誤検出 | 30.7 | 31.3 | 28.0 |
| Bicycle/(39,5)林/50 | 消失 | 16.0 | 14.7 | 24.0 |
| | 誤検出 | 28.0 | 21.3 | 24.0 |
| Susie/(26,10)右頬/10 | 消失 | 14.0 | 17.3 | 20.7 |
| | 誤検出 | 30.7 | 27.3 | 28.0 |

表1, 2から、一つのMBだけではかなり高い確で誤ることがわかる。また、あまりビットレー画像やMPEG復号前後にはよらない結果となた。そもそも提案方式での誤りは、DCT係数揺による非定常性が、画像信号が元来持っている定常性や、動き補償や適応量子化等の符号化プセスにおける非定常性に紛れたり、消されたり

ることによって起きる。これらの外乱である非定常性は表 1,2 のパラメータとは直接には無相関であるため、表 1,2 において明確な特性の出ない理由と思われる。

次に第 1 階層については、10 フレーム周期のテンプレートを用いた。フレームごとの埋め込み位置は、MB 位置を MB ごとにインクリメントする x, y 座標で表現すると、(5,4) (18,25) (26,10) (23,10) (35,2) (36,22) (10,28) (14,14) (15,4) (6,26) とした。このとき、MPEG ビットストリームおよび MPEG 復号後について、安定して同期を回復できる検査フレーム長をシミュレーションによって求めた結果を表 3 に示す。

表 3　同期回復に必要なフレーム数
(MPEG ビットストリーム)

| 画像 | ビットレート(Mbit/s) | | |
|---|---|---|---|
| | 15 | 8 | 4 |
| Flower | 20 | 30 | 40 |
| Bicycle | 10 | 10 | 30 |
| Susie | 10 | 20 | 20 |

表 4　同期回復に必要なフレーム数
(MPEG 復号後)

| 画像 | ビットレート(Mbit/s) | | |
|---|---|---|---|
| | 15 | 8 | 4 |
| Flower | 20 | 10 | 10 |
| Bicycle | 10 | 10 | 10 |
| Susie | 10 | 10 | 10 |

この結果で、MPEG ビットストリームにおいてビットレートが低いときに、より多くのフレーム数を要しているのは、not-Coded ブロックが増えるために透かし判定に利用できる MB 数が減ることによる。

第 2 階層の埋め込みには、各フレームグループ内でテンプレートを用いて、フレームごとに異なる MB に埋め込みを行うこととした。使用した MB 座標は順に(40,5) (30,22) (8,20) (25,18) (6,6) (8,14) (31,6) (30,25) (15,4) (39,15) (7,20) (22,27) (24,7) (40,20) (4,8)である。このとき、フレームグループごとに 1 または 0 を(1001101011)および(0110010100)なる 10 ビットパターンとして埋め込みを行った。上記の二通りのビットパターンのいずれの場合についても、正確に抽出するのに必要なフレーム数をシミュレーションにより調べた。

表 5　情報抽出に必要なフレーム数
(MPEG ビットストリーム)

| 画像 | ビットレート(Mbit/s) | | |
|---|---|---|---|
| | 15 | 8 | 4 |
| Flower | NG | NG | NG |
| Bicycle | 140 | 140 | NG |
| Susie | 60 | 140 | NG |

表 6　情報抽出に必要なフレーム数
(MPEG 復号後)

| 画像 | ビットレート(Mbit/s) | | |
|---|---|---|---|
| | 15 | 8 | 4 |
| Flower | 150 | 90 | 110 |
| Bicycle | 130 | 130 | 130 |
| Susie | 70 | 70 | 70 |

表 5 において NG とあるのは、150 フレームを費やしても抽出できなかったことを示している。MPEG ビットストリーム上の抽出で、ビットレートが下がるほど多くのフレーム数が必要となったり、抽出ができなくなったりするのは、第 1 階層の場合と同様に not-Coded ブロックが増えて、判定に利用できるブロック数が減少してしまうことによる。

## 5. 考察

提案方式では統計的に埋め込みの有無の判定を行っているため、その判定の確実さに関する評価が必要である。いま、埋め込みを行った場合を 1、埋め込みを行っていない場合を 0 と表現すると、第 1 階層および第 2 階層における抽出は、元々すべて 0 または 1 の系列が確率的に変化した観測結果に基づいて元の系列がどちらであったかを判定する問題となる。このとき、ある観測結果が元々すべて 1 であると判定する際の危険度は、元が本当はすべて 0 であった確率で評価されることになる。逆に言うと、例えば危険度 5%で判定を行うた

めには、元がすべて0である確率が5%以下になるまで観測個数を増やして1の観測比率を高めればよいということになる。この観測はベルヌーイ試行であるので、確率は(2)式で示される。

$$P(k)=\binom{n}{k}p^k(1-p)^{n-k} \qquad (2)$$

ここで、nは観測個数、kは1の観測個数、pは0が1に変化する確率である。第1階層、第2階層の抽出時には、単純な多数決決定に加えて、その精度の判定に(2)式を利用することができる。なお、確率pの値については、表1, 2の結果を利用すればよい。

次に、提案方式の耐攻撃性について考察する。まず、MPEGによる圧縮の影響は、実験結果において圧縮による画質劣化が生じるほどビットレートを下げても誤り確率が変わらないことから、ほとんどないと言える。画像処理に関する耐性は、低次の DCT 係数への影響が少ないものに対しては強いと思われるが、画素位置のずらしには弱いと思われる。このような処理に対して耐性を持たせるには画面全体を使って薄く情報を埋め込む方式が必要となるが、埋め込み・抽出処理に必要な演算量を考えると現時点では適した方式はなく、今後の検討が必要である。なお、提案方式に対する最も簡単な攻撃方法として、フレーム間引きや順序の入れ替えが考えられる。これは提案方式の第1階層、第2階層の埋め込みで前提としているフレームの連続性を崩す攻撃法である。この攻撃への対策は、ある程度連続したフレームをひとかたまりとして扱って、このかたまり内では埋め込み DCT ブロック位置を同一にして冗長度を増すような方法になると考えられる。

## 6. まとめ

動画像の特性を考慮した新しい統計的な電子透かし埋め込み・抽出方式を提案した。提案方式の特徴は、MPEG ビットストリームを復号することなく透かしの抽出が可能であることと、処理フレーム数を増やすことで抽出情報量が増えたり、情報の精度が向上するというスケーラビリティを実現したことである。

今後の課題は、埋め込み値の適応的変化による最適化とフィールド DCT への対応である。本稿では、簡単のため埋め込み値を固定としていた。DCについても、埋め込み時の DCT と整合性を持たるため MPEG での圧縮にはフレーム DCT のみ用いていたが、一般に MPEG ではフィールド DCとフレーム DCT が適応的に切り替えて使用される。また、誤り確率の低減、耐攻撃性の強化も取り組まなければならない課題である。


## 謝辞

日ごろご指導いただく（株）KDD 研究所 [illegible] 所長、鈴木、山本副所長、羽鳥取締役に感謝いたします。


## 参考文献


[1] 松井:"電子透かし技術とその評価項目", 画電子学会誌, Vol.27, No.5, pp.483-491 (199

[2] 中村, 小川, 高嶋: "ディジタル動画像の著作保護のための周波数領域における電子透か方式", 暗号と情報セキュリティシンポジウ SCIS'97-26A (1997).

[3] 大西, 岡, 松井:"PN 系列による画像への透し署名法", 暗号と情報セキュリティシンポウム SCIS'97-26B (1997).

[4] 福岡, 松井:"フーリエ変換による画像への電透かしの一方法", 暗号と情報セキュリティンポジウム SCIS'98-3.2.C (1998).

[5] ISO/IEC JTC1/SC29/WG11: MPEG93/4 (Test Model 5).